Trajtimi i Incidenteve

CSIRTs

Vështrim i përgjithshëm i CSIRT

- Ekipi i Reagimit të Incidentit të Sigurisë Kompjuterike (CSIRT) është një grup i gjetur shpesh brenda një organizate që ofron shërbime dhe funksione për të siguruar pasuritë e kësaj organizate.

- Një CSIRT:
  - Përgjigjet ndaj incidenteve që kanë ndodhur tashmë.
  - Ofron shërbime proaktive dhe funksione të tilla si testimi i depërtimit, zbulimi i ndërhyrjeve, apo edhe trajnimi për vetëdijesimin e sigurisë.

CSIRTs

Llojet e CSIRTs

- Ka shumë lloje të ndryshme të CSIRTs dhe organizatave të lidhura:
  - I brendshëm - përdoret në banka, spitale, universitete etj.
  - Kombëtare - merret me incidente për një vend
  - Qendra e koordinimit - trajtimi i incidenteve nëpër CSIRT të shumëfishta
  - Qendrat e analizës - të dhëna nga shumë burime për të identifikuar tendencat
  - Ekipet e shitësit - riparimi për dobësitë në hardware / software
  - Ofruesit e shërbimeve të sigurisë të menaxhuara - një shërbim i bazuar në tarifë

CSIRTs

CERT

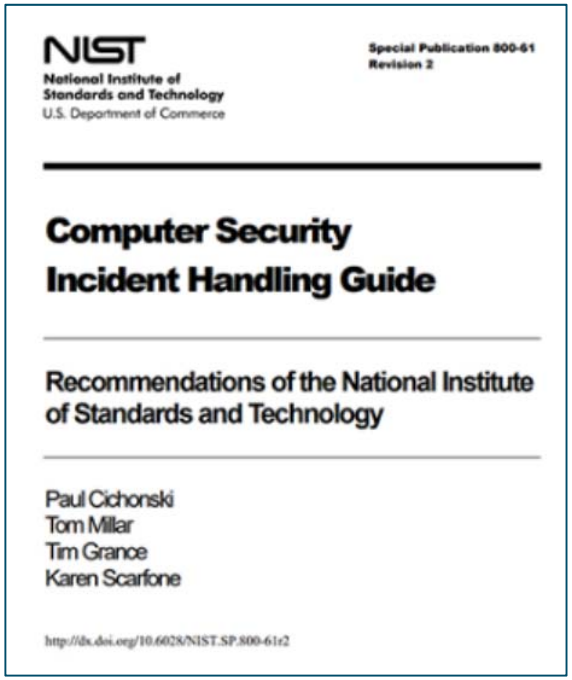
- Ekipi i reagimit emergjent kompjuterik (CERT) është një akronim i markës tregtare i zotëruar nga Universiteti Carnegie Mellon.
- Një CERT siguron ndërgjegjësimin e sigurisë, praktikat më të mira dhe informacionin mbi cenueshmërinë e sigurisë, por nuk i përgjigjet incidenteve të sigurisë.
- Vende të tjera kanë kërkuar leje për të përdorur akronimin CERT.

NIST 800-61r2

Krijimi i një Aftësie të Përgjigjes së Incidentit

- NIST "Udhëzues për Trajtimin e Incidenteve të Sigurisë Kompjuterike" Publikimi Special 800-61, rishikimi 2 (800-61r2) ofron udhëzime për:
  - Trajtimi i incidentit
  - Analizimi i të dhënave të lidhura me incidentet
  - Përcaktimi i përgjigjes së duhur për secilin incident

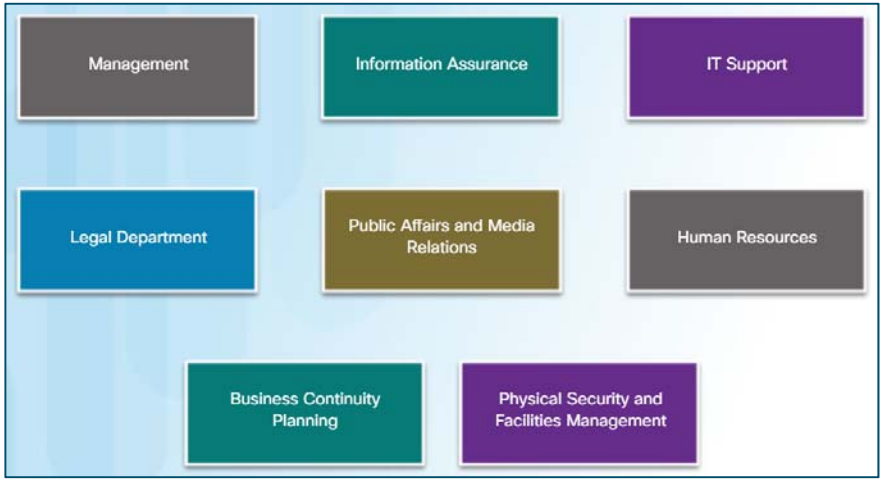
- NIST rekomandon krijimin e një aftësie për përgjigjen e incidenteve të sigurisë në kompjuter (CSIRC) dhe krijimin e:
  - **Politikat e Reagimit të Incidentit**
  - **Planet e Reagimit të Incidentit**
  - **Procedurat e Përgjigjeve të Incidentit**



NIST 800-61r2

Palët e Interesuara për përgjigje ndaj incidentit

- Grupet dhe individët e mëposhtëm mund të përfshihen edhe në trajtimin e incidenteve.

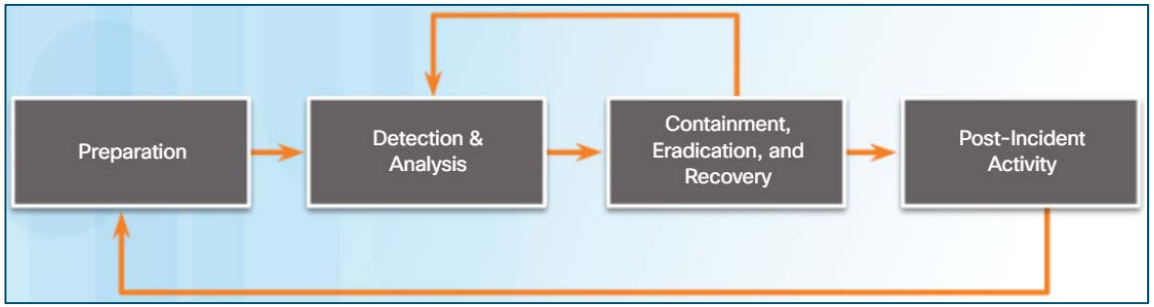


- Është e rëndësishme të sigurohet bashkëpunimi i tyre para se të ndodhë një incident, pasi ekspertiza dhe aftësitë e tyre mund të ndihmojnë CSIRT-në për të trajtuar ngjarjen shpejt dhe saktë.

NIST 800-61r2

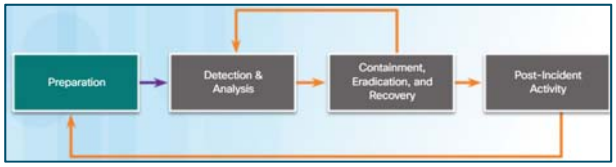
Cikli i Jetës së Përgjigjes ndaj Incidentit në NIST

- NIST përcakton katër hapat e mëposhtëm në ciklin e jetës së procesit të reagimit të incidentit:
  - Përgatitja - Anëtarët e CSIRT-it trajnohen se si t'i përgjigjen një incidenti.
  - Zbulimi dhe analiza - Nëpërmjet monitorimit të vazhdueshëm, CSIRT identifikon, analizon dhe vërteton shpejt një incident.
  - Përmbarimi, çrrënjosja dhe rimëkëmbja - CSIRT zbaton procedurat për të përmbajtur kërcënimin, për të zhdukur ndikimin në asetet organizative dhe për të përdorur rezerva për të rivendosur të dhënat dhe softuerin.
  - Aktivitetet pas incidentit - CSIRT pastaj dokumenton se si është trajtuar incidenti, rekomandon ndryshimet për përgjigjen e ardhshme dhe specifikon se si të shmanget një përsëritje.



NIST 800-61r2

Përgatitja

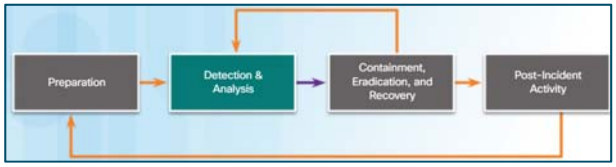


- Faza e përgatitjes është kur CSIRT është:
  - Krijuar dhe trajnuar
  - Mjetet dhe asetet që do të nevojiten për të hetuar incidentet janë të blera dhe të vendosura.

- Në vijim janë shembuj të veprimeve që ndodhin edhe gjatë fazës përgatitore:
  - Proceset organizative janë krijuar për të adresuar komunikimin ndërmjet njerëzve në ekipin e reagimit.
  - Lehtësitë për të strehuar ekipin e reagimit dhe SOC janë krijuar.
  - Hardware dhe softueri i domosdoshëm për analiza dhe zbutje të incidentit është fituar.
  - Vlerësimet e rrezikut përdoren për të zbatuar kontrolle që do të kufizojnë numrin e incidenteve.
  - Validimi i pajisjeve të sigurisë dhe vendosjes së softuerit kryhet në pajisjet.
  - Materialet e trajnimit për ndërgjegjësimin e përdoruesve janë zhvilluar.

NIST 800-61r2

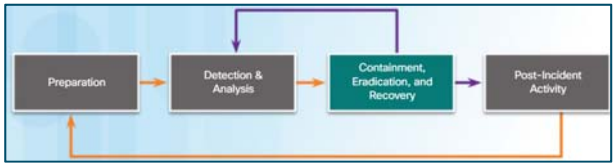
Zbulimi dhe Analizimi



- Llojet e ndryshme të incidenteve do të kërkojnë përgjigje të ndryshme dhe organizatat duhet të përgatiten për incidente nga vektorë të ndryshëm të sulmeve duke përfshirë Web, Email, humbje ose vjedhje, imitim, deprimim ose media.
- Disa incidente janë të lehta për t'u zbuluar, ndërsa të tjerët mund të mos zbulohen për muaj të tërë.
  - Ka mënyra të zbulimit të automatizuar si softueri antivirus ose IDS.
  - Ekzistojnë edhe zbulime manuale përmes raporteve të përdoruesve.
  - Ka dy kategori për shenjat e një incidenti; paraardhës dhe tregues.
- Analiza e incidentit është e vështirë, sepse jo të gjithë treguesit janë të sakta dhe CSIRT duhet të reagojë shpejt për të vërtetuar dhe analizuar incidentet.
- Njoftimi i incidentit është kur një incident është analizuar dhe prioritizuar, ekipi i reagimit të incidentit duhet të njoftojë individët e duhur në mënyrë që të gjithë ata që duhet të jenë të përfshirë do të luajnë rolet e tyre.

NIST 800-61r2

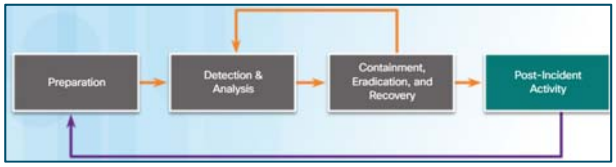
Përmbarimi, Zhdukja dhe Rimëkëmbja



- Kontrasti siguron që incidenti të mos vazhdojë.
  - Llojet e ndryshme të incidenteve do të kërkojnë strategji të ndryshme.
  - Për çdo lloj incidenti, duhet të krijohet një strategji e kontrollit dhe të zbatohet.
  - Gjatë një incidenti, dëshmitë duhet të mblidhen dhe të dokumentohen në mënyrë të qartë dhe koncize për hetime të mëvonshme nga autoritetet.
- Zhdukja po identifikon të gjithë ushtritë që kanë nevojë për riparim dhe të gjitha efektet e incidentit të sigurisë duhet të eliminohen.
  - Dobësitë e shfrytëzuara duhet të korrigjohen ose të rregullohen në mënyrë që incidenti të mos ndodhë përsëri.
- Rimëkëmbja e hostëve kërkon backup të pastër dhe të fundit, ose ato do të duhet të rindërtohen me mediat e instalimit.

NIST 800-61r2

Faza e Aktivitetit pas Incidentit



- Është e rëndësishme të kryhet një post-mortem dhe të takohen periodikisht me të gjitha palët e përfshira për të diskutuar ngjarjet që ndodhën dhe veprimet e të gjithë individëve gjatë trajtimit të incidentit.
- Pas një incidenti të madh është trajtuar, organizata duhet të mbajë një takim "mësime të nxjerra" në:
  - Shqyrtoni efektivitetin e procesit të trajtimit të incidenteve.
  - Identifikoni forcimin e nevojshëm të nevojshëm për kontrollet dhe praktikat ekzistuese të sigurisë.

NIST 800-61r2

Mbledhja dhe Ruajtja e të Dhënave të Incidentit

- Në mbledhjet 'mësimet e nxjerra', të dhënat e mbledhura mund të përdoren për:
  - Përcaktoni koston e një incidenti për arsye të buxhetit.
  - Përcaktoni efektivitetin e CSIRT.
  - Identifikoni dobësitë e mundshme të sigurisë në të gjithë sistemin.
- NIST Special Publication 800-61 ofron shembuj të kryerjes së një vlerësimi objektiv të një incidenti.
- Duhet të ekzistojë një politikë e mbajtjes së provave që përshkruan se sa dëshmi të një incidenti duhet të mbahen.
  - Dëshmia shpesh ruhet për shumë muaj apo shumë vite pas një incidenti.
  - Arsyet që ndikojnë në mbajtjen e provave përfshijnë ndjekjen, llojin e të dhënave dhe koston e ruajtjes.

NIST 800-61r2

Kërkesat e Raportimit dhe Ndarja e Informacionit

- Një organizatë mund të ketë kërkesa për raportim.
  - Mund të ketë rregulla qeveritare që organizata duhet t'i përmbahet.
  - Menaxhmenti mund të duhet gjithashtu të raportojë tek palët e interesit, klientët, shitësit, partnerët etj.
- NIST rekomandon që organizatat të ndajnë informacionin e incidentit me VERIS, megjithatë:
  - Plani i koordinimit të incidenteve me palët e jashtme përpara incidenteve.
  - Konsultohuni me departamentin ligjor para fillimit të ndonjë përpjekjeje koordinimi.
  - Kryen ndarjen e informacionit të incidentit gjatë gjithë ciklit jetësor të përgjigjes së incidentit.
  - Përpiquni të automatizoni sa më shumë procesin e shkëmbimit të informacionit.
  - Bilanci përfitimet e ndarjes së informacionit me të metat e ndarjes së informacionit të ndjeshëm.
  - Ndani sa më shumë informacionin e duhur të incidentit me organizatat e tjera.

Përmbledhje

- Zinxhiri Killues Cyber përshkruan hapat që një sulmues duhet të kryejë për të përmbushur qëllimin e tyre. Këto hapa janë zbulimi, armatimi, dorëzimi, shfrytëzimi, instalimi, komanda dhe kontrolli.
- Modeli Diamond i ndërhyrjes përdoret për të diagramuar një seri ngjarjesh ndërhyrëse. Është ideale për të treguar se si kundërshtari kalon nga një ngjarje në tjetrën.
- Modeli i Diamantit ka 4 pjesë të përdorura për të përfaqësuar një incident ose ngjarje sigurie: kundërshtari, aftësia, infrastruktura dhe viktima.
- VERIS mund të përdoret për të paraqitur detajet e incidentit të sigurisë në VCDB për përdorim në komunitet.
- Elementet e nivelit të lartë të skemës VERIS përfshijnë vlerësimin e ndikimit, zbulimin dhe përgjigjen, përshkrimin e incidentit, demografinë e viktimave dhe ndjekjen e incidenteve.
- Një CSIRT është një grup që ofron shërbime dhe funksione në përgjigje të incidenteve të sigurisë.
- Llojet e CSIRT përfshijnë qendra të brendshme, kombëtare, koordinimi, qendra analitike, skuadra të shitësve dhe ofruesit e shërbimeve të sigurisë të menaxhuara.
- CERT është një akronim i markës tregtare në pronësi të Universitetit Carnegie Mellon, por përdoret me leje nga vende të tjera. Një CERT siguron ndërgjegjësimin e sigurisë, praktikat më të mira dhe informacionin e cenueshmërisë së sigurisë; një CERT nuk i përgjigjet incidenteve të sigurisë.
- Standardi NIST 800-61r2 ofron udhëzime për trajtimin e incidenteve. Fazat e një cikli jetësor të procesit të reagimit të incidentit janë përgatitje; zbulimin dhe analizën; kontrollin, zhdukjen dhe rikuperimin; dhe aktivitetet pas incidentit.